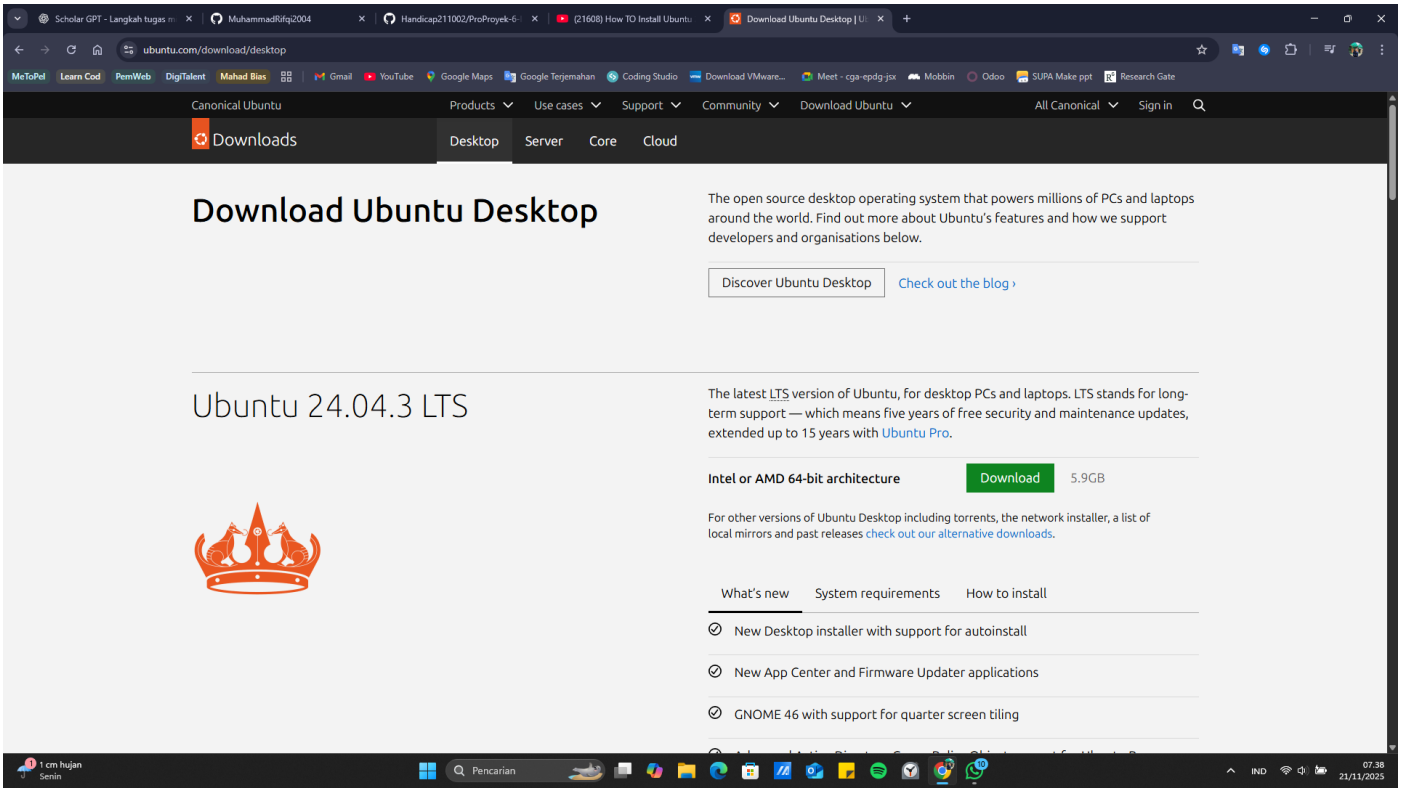
Projek 6: Implementasi IDS (Instruction Detection System) dengan Snort / Suricata

Nama Kelompok :

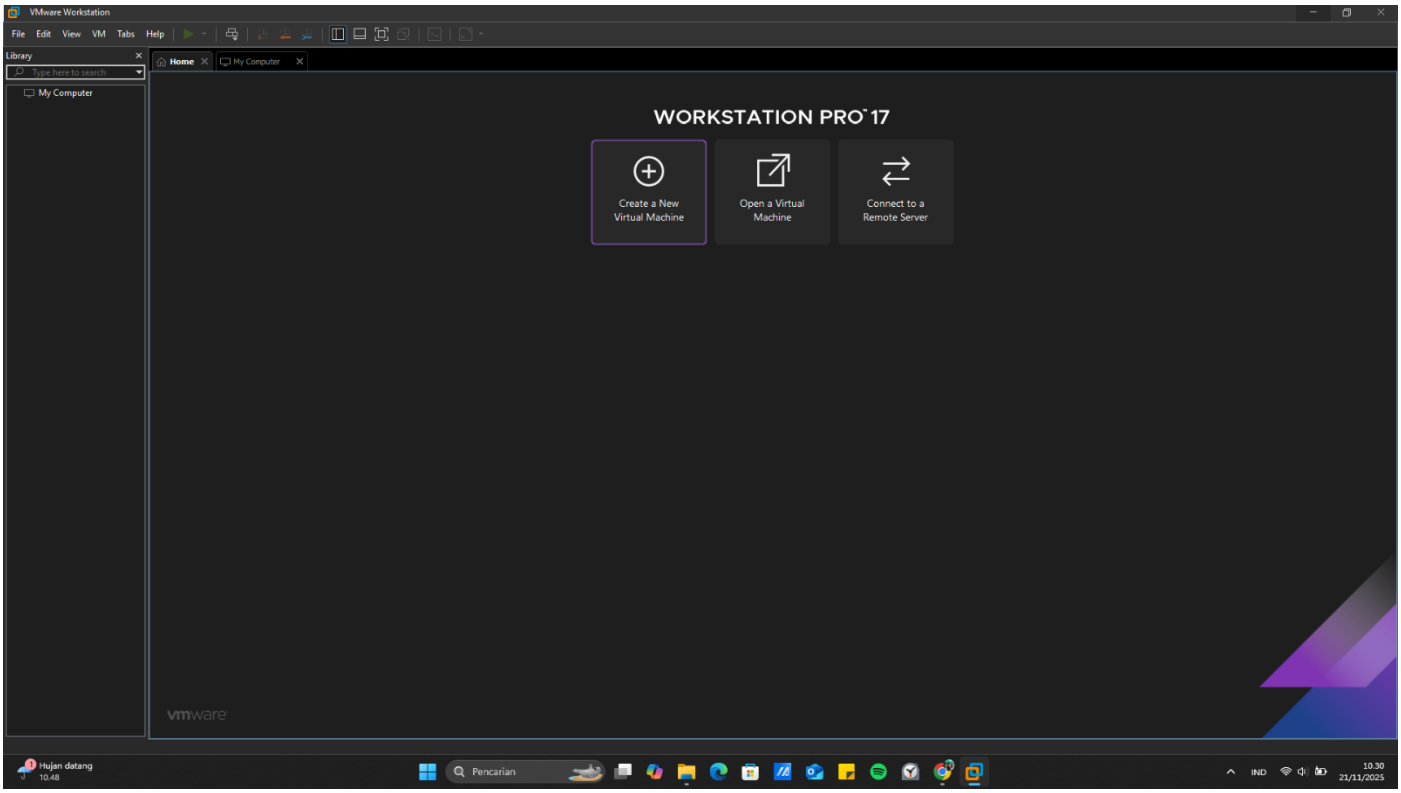
- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah

Instalasi Linux

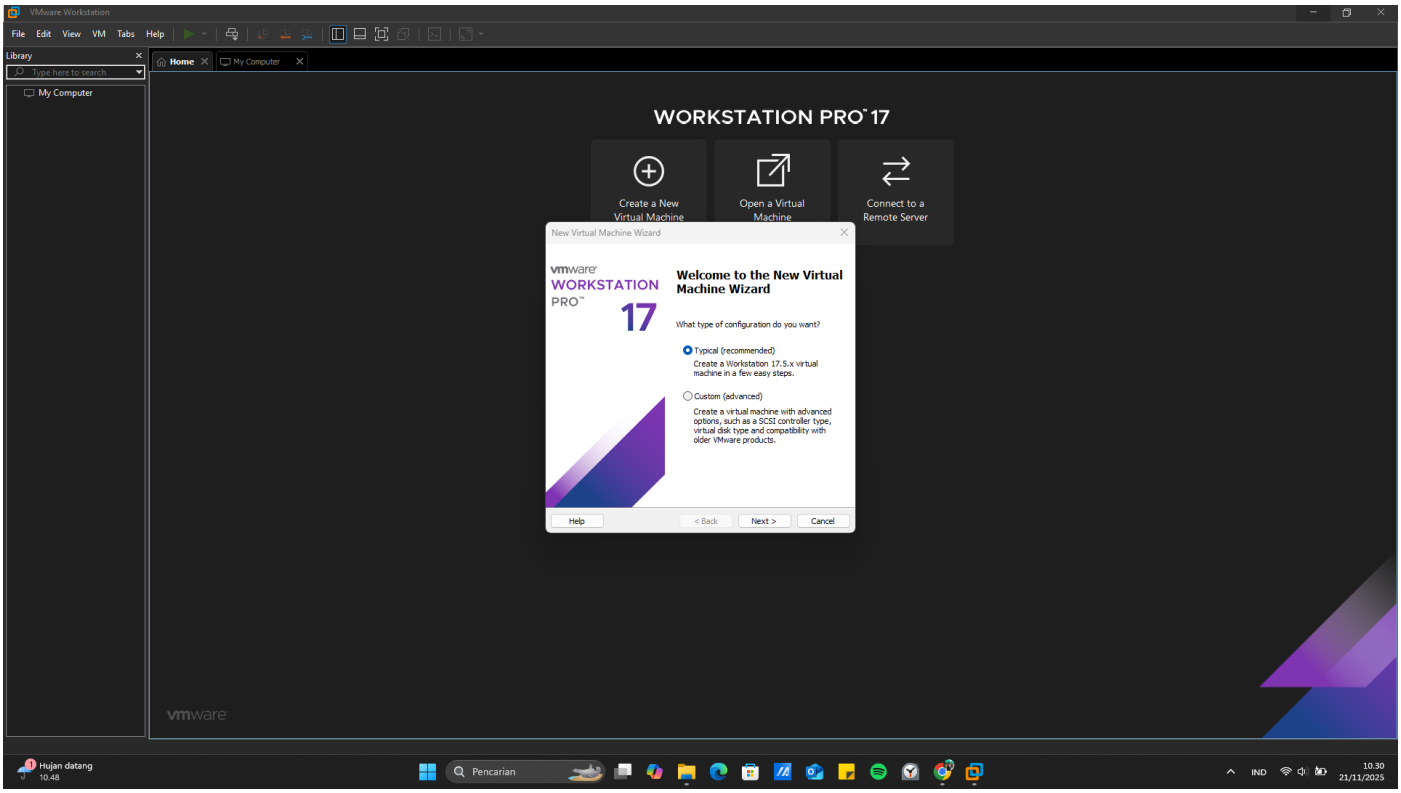
1. Install Ubuntu Server / Desktop, disini saya memilih Desktop karena lebih gampang untuk pemula



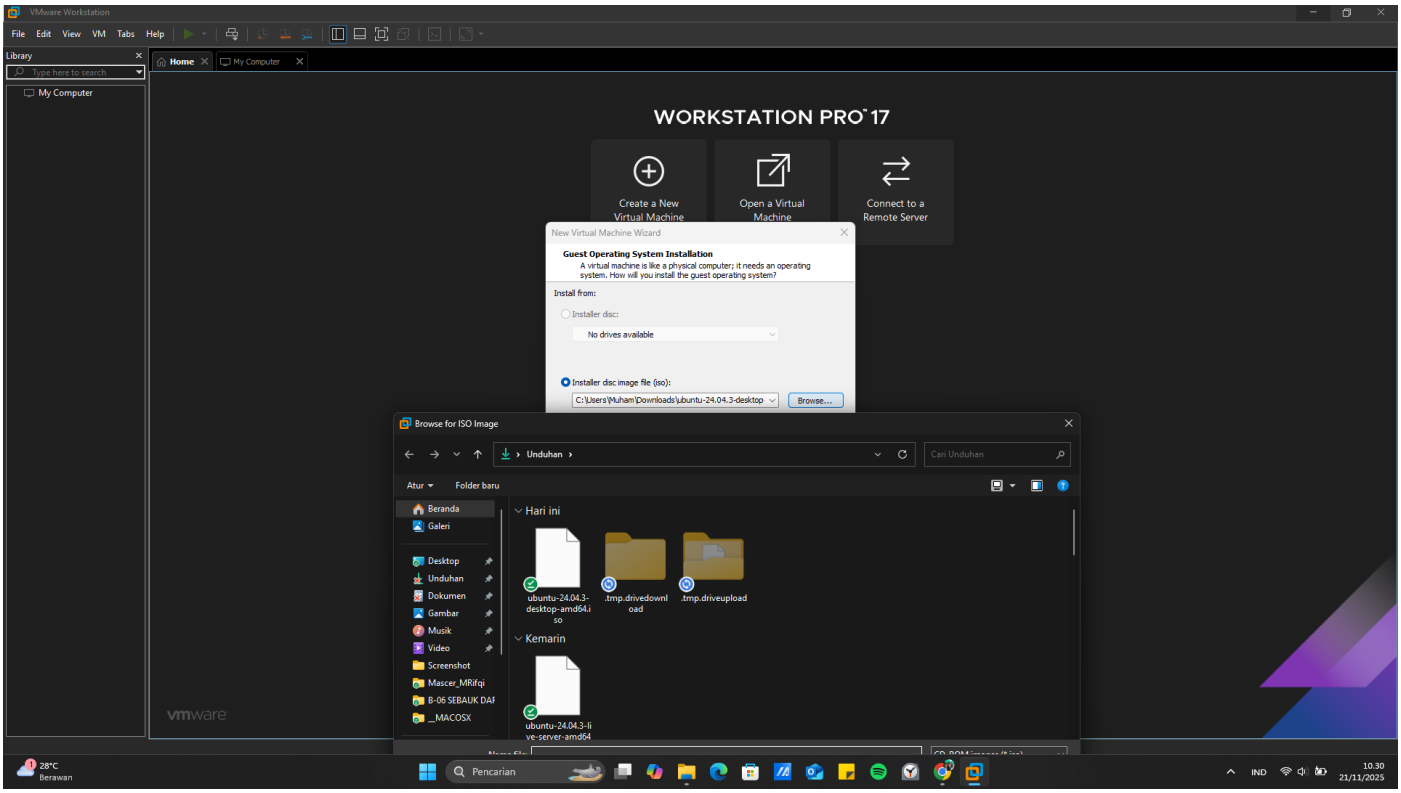
2. Kemudian masuk ke dalam VMWare dan klik create a new VM



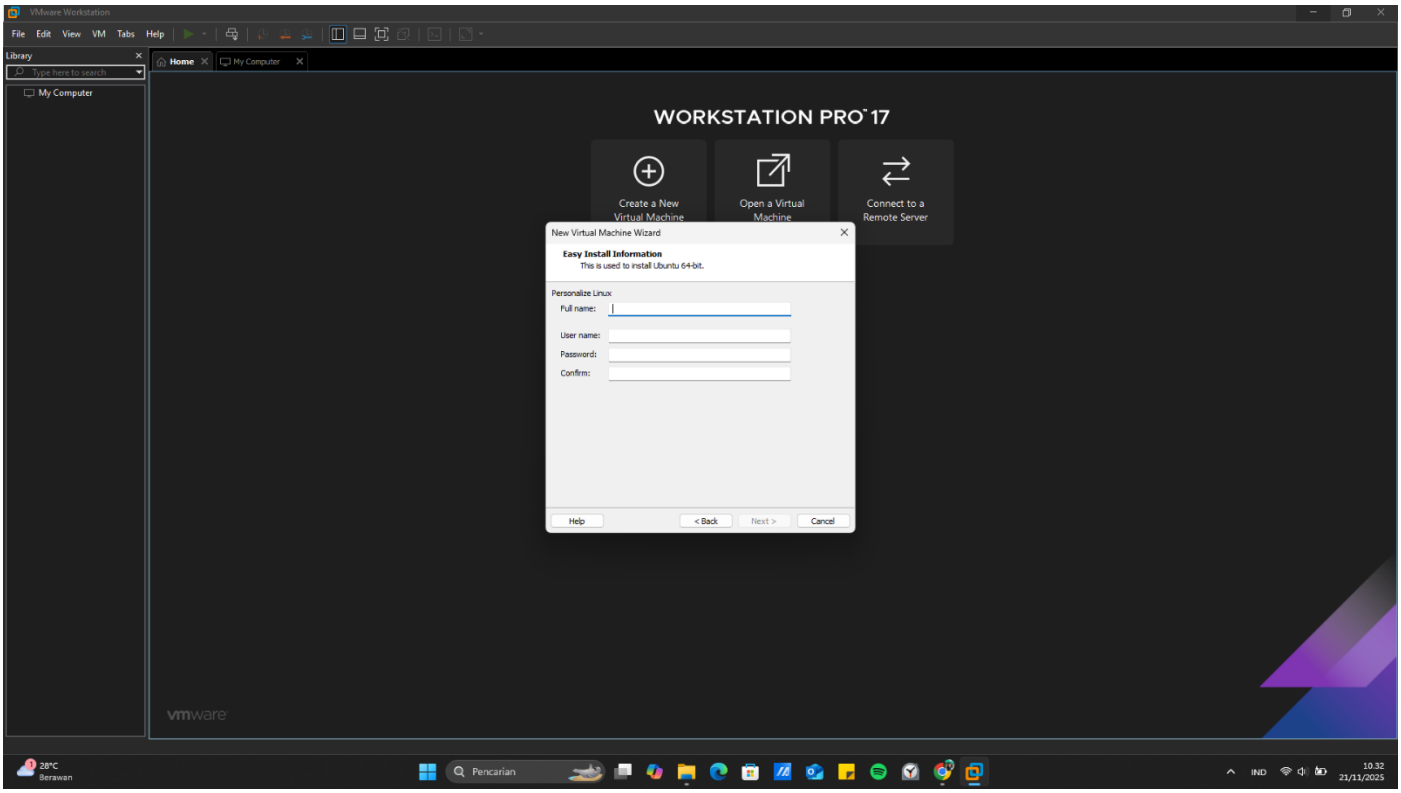
3. Untuk pemula disarankan memilih typical (recomended) agar bisa dipilihkan oleh sistem



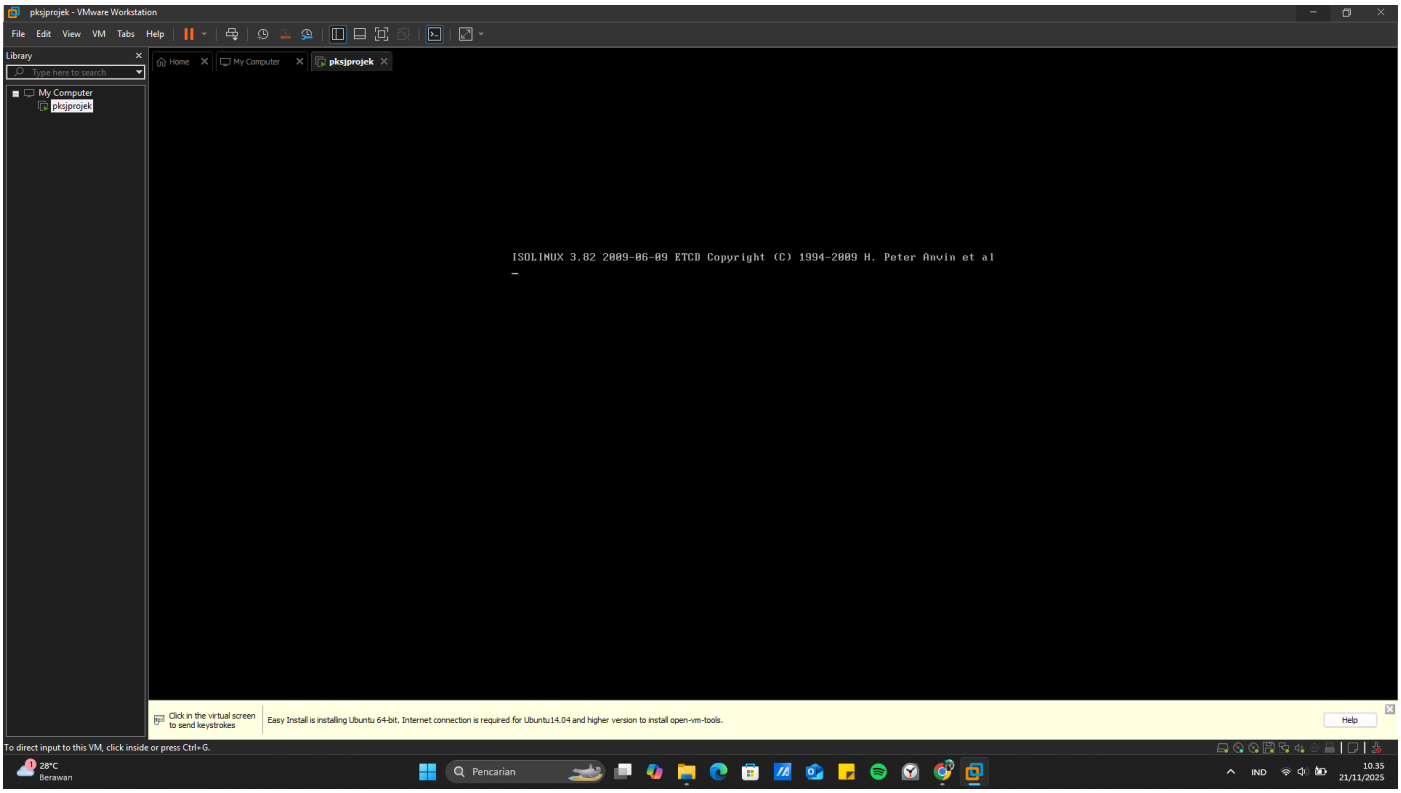
4. Masukkam file Ubuntu yang sudah di download tadi



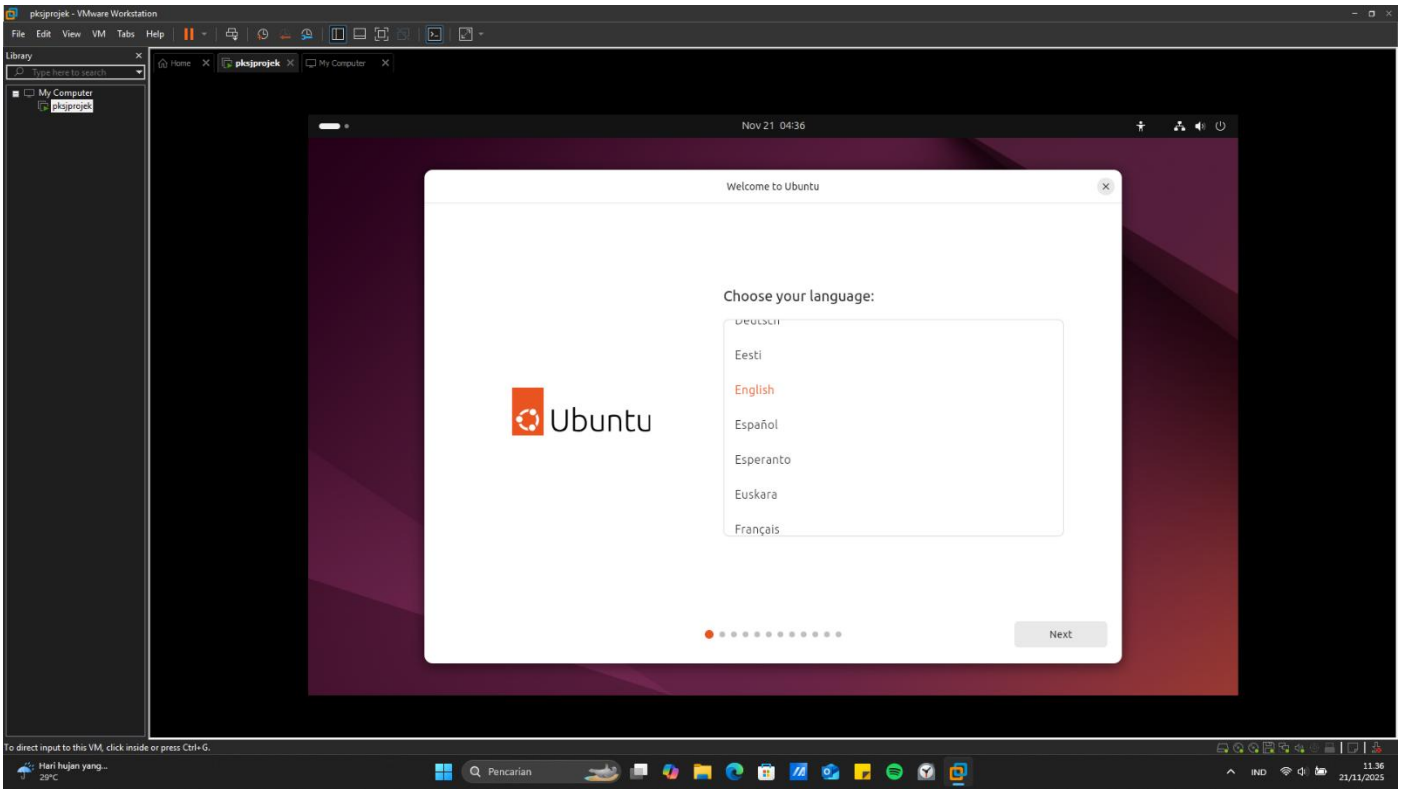
5. Buat akun terlebih dahulu



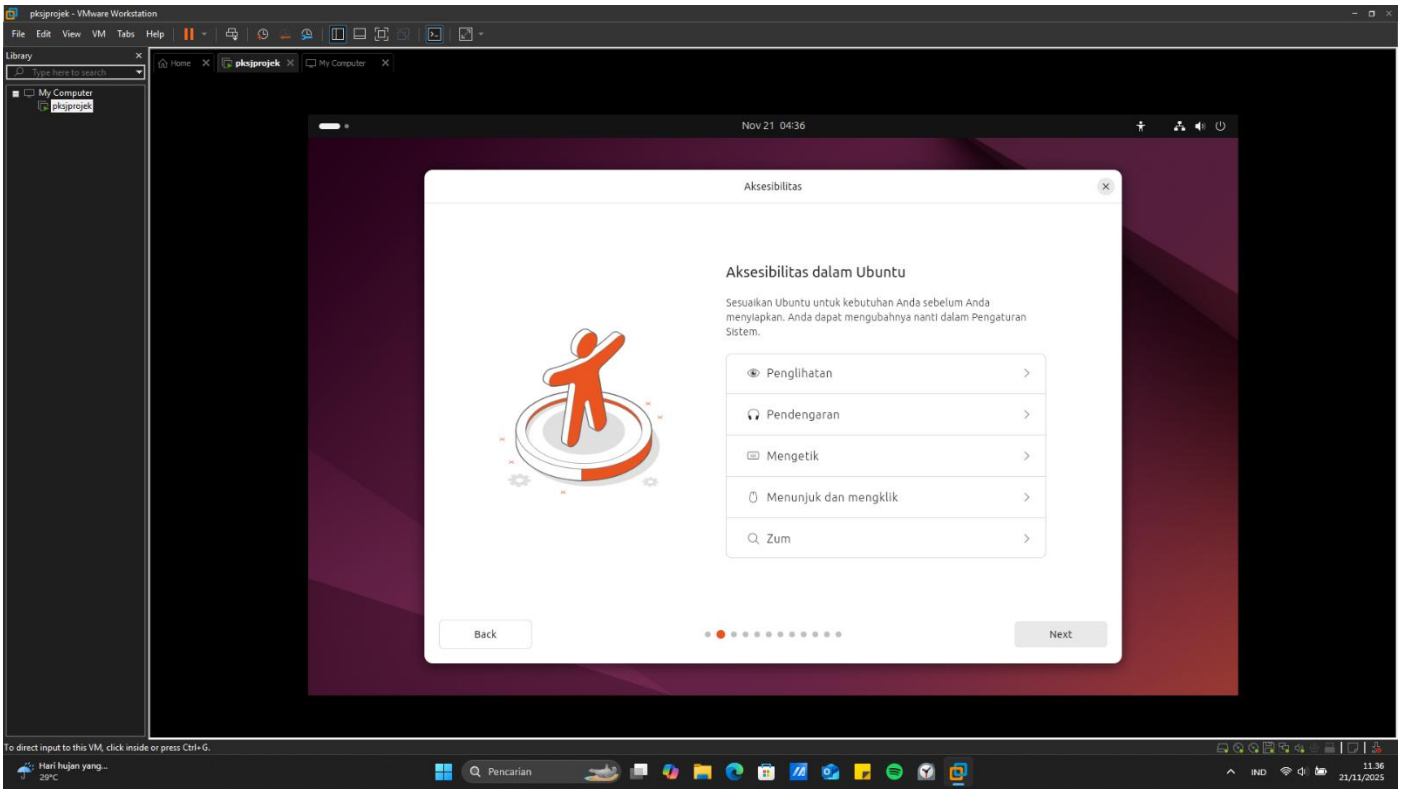
6. Ketika sudah muncul seperti ini, biarkan saja, karena mesin sedang memproses



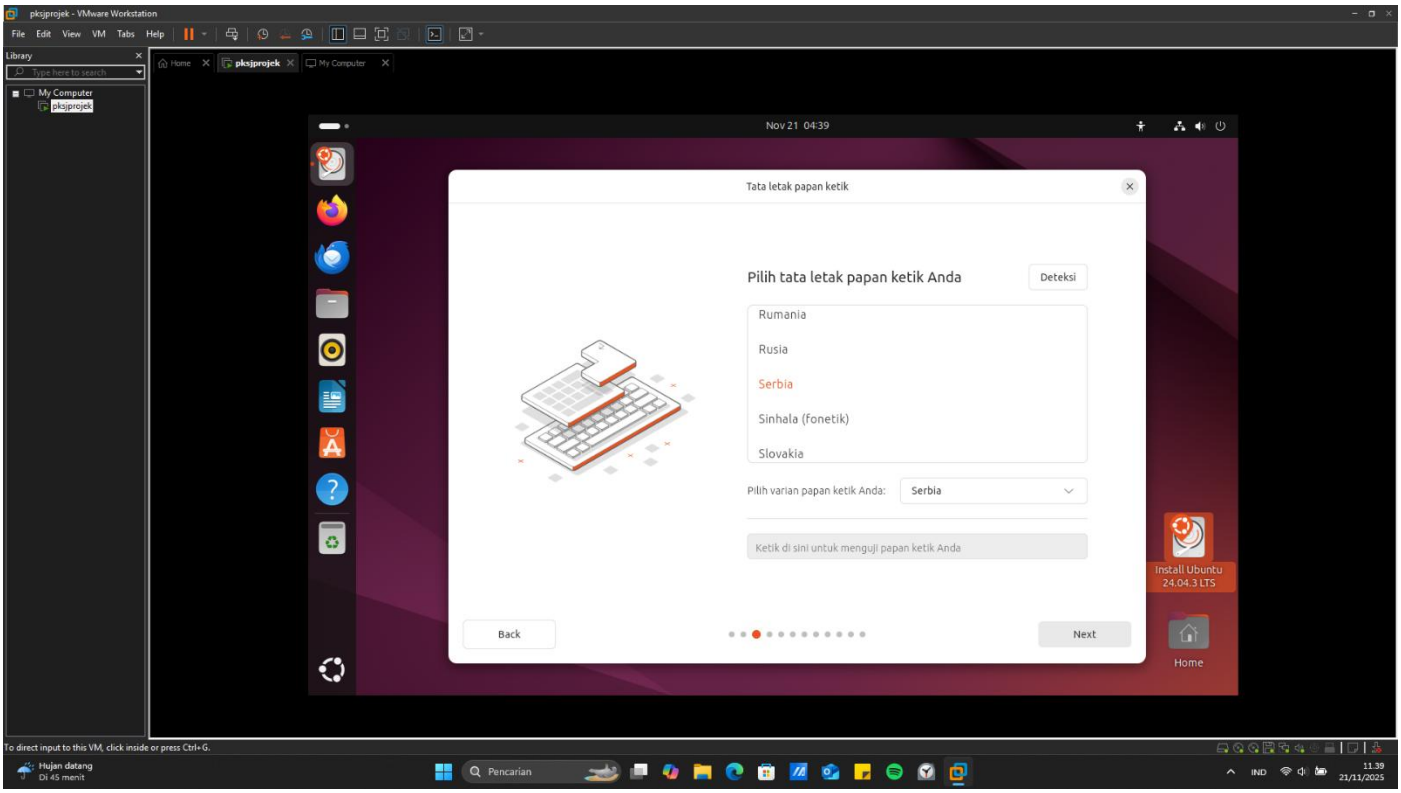
7. Pilihlah bahasa yang akan kamu gunakan



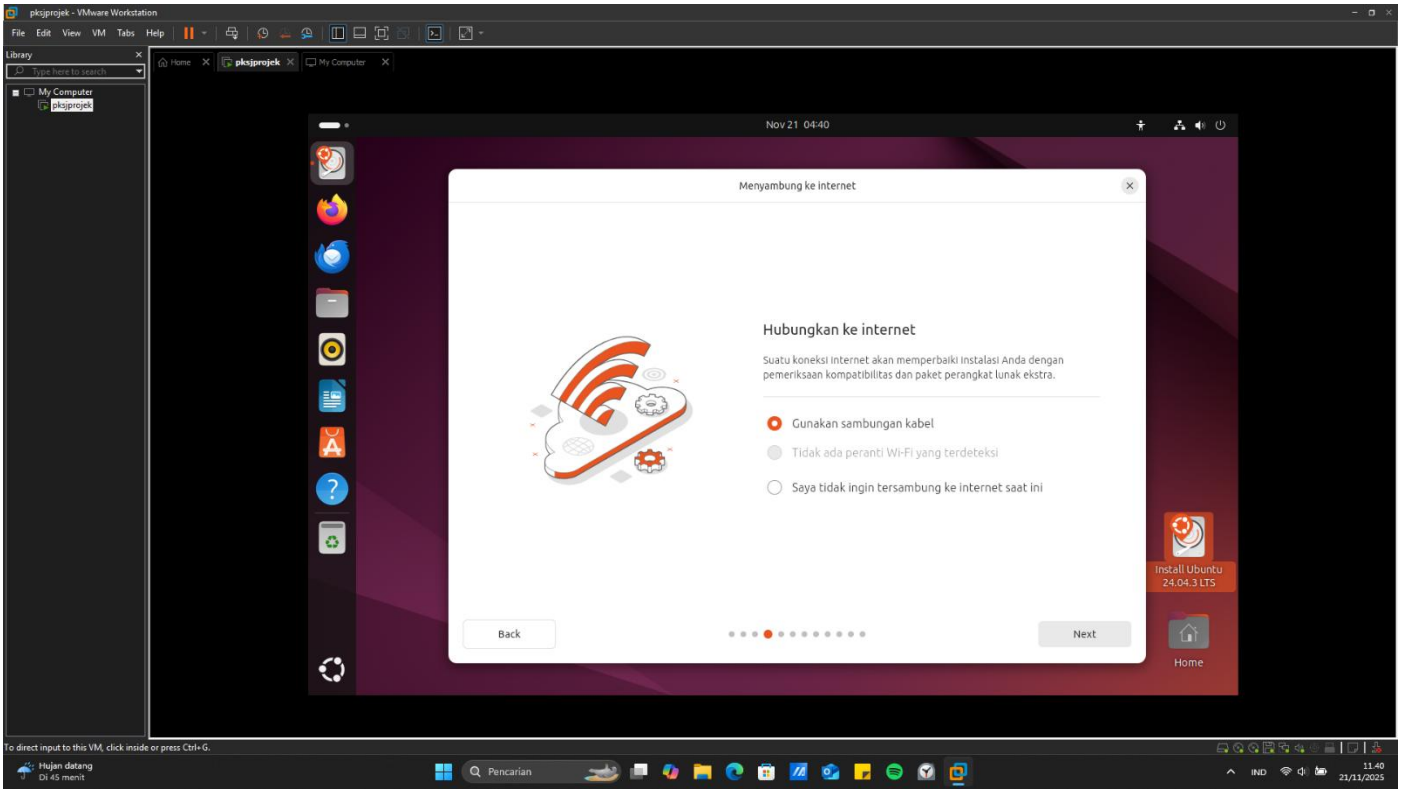
8. Lanjut aja dengan menekan next



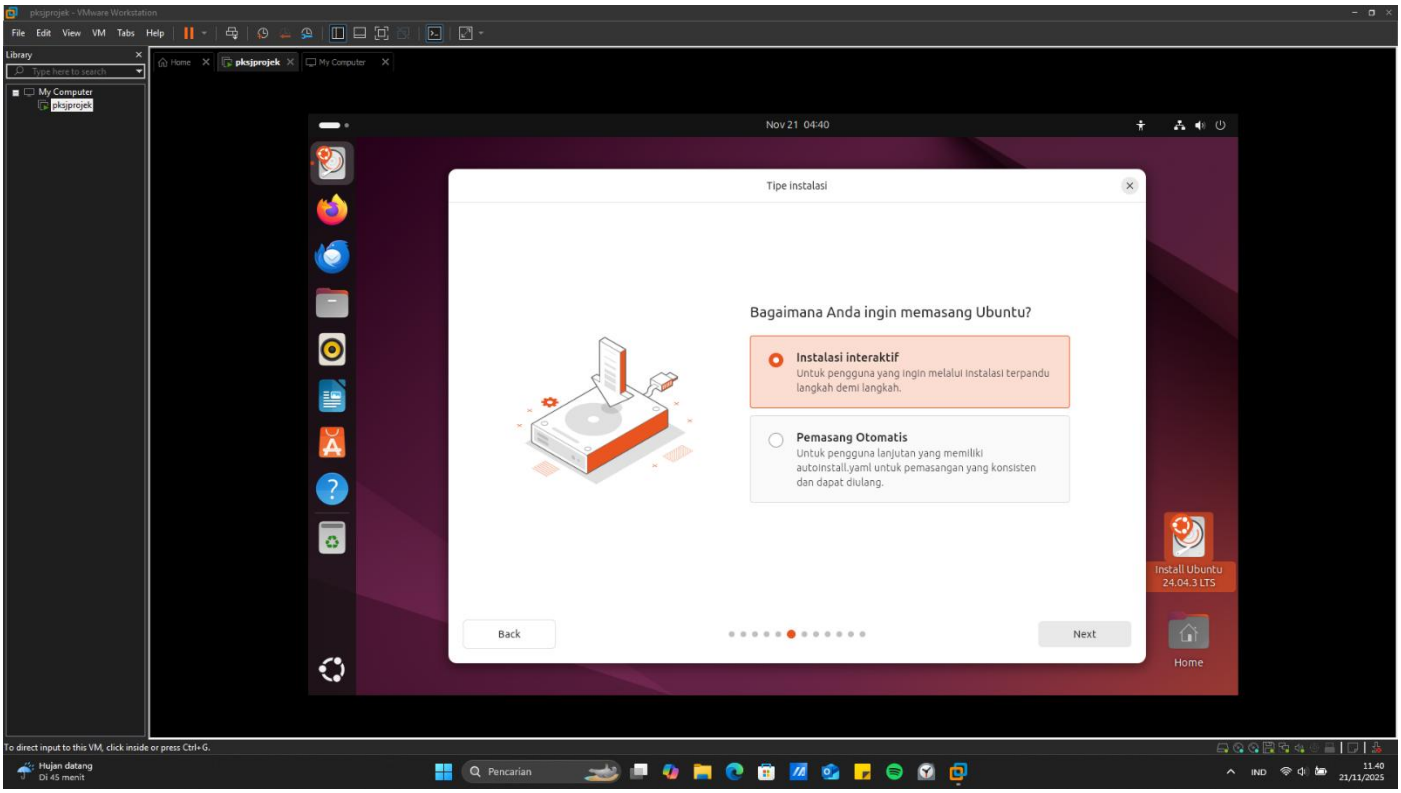
9. Kalua kalian terbiasa dengan keyboard dengan urutan huruf QUERTYUIOP{[}], disarankan memilih Inggris US



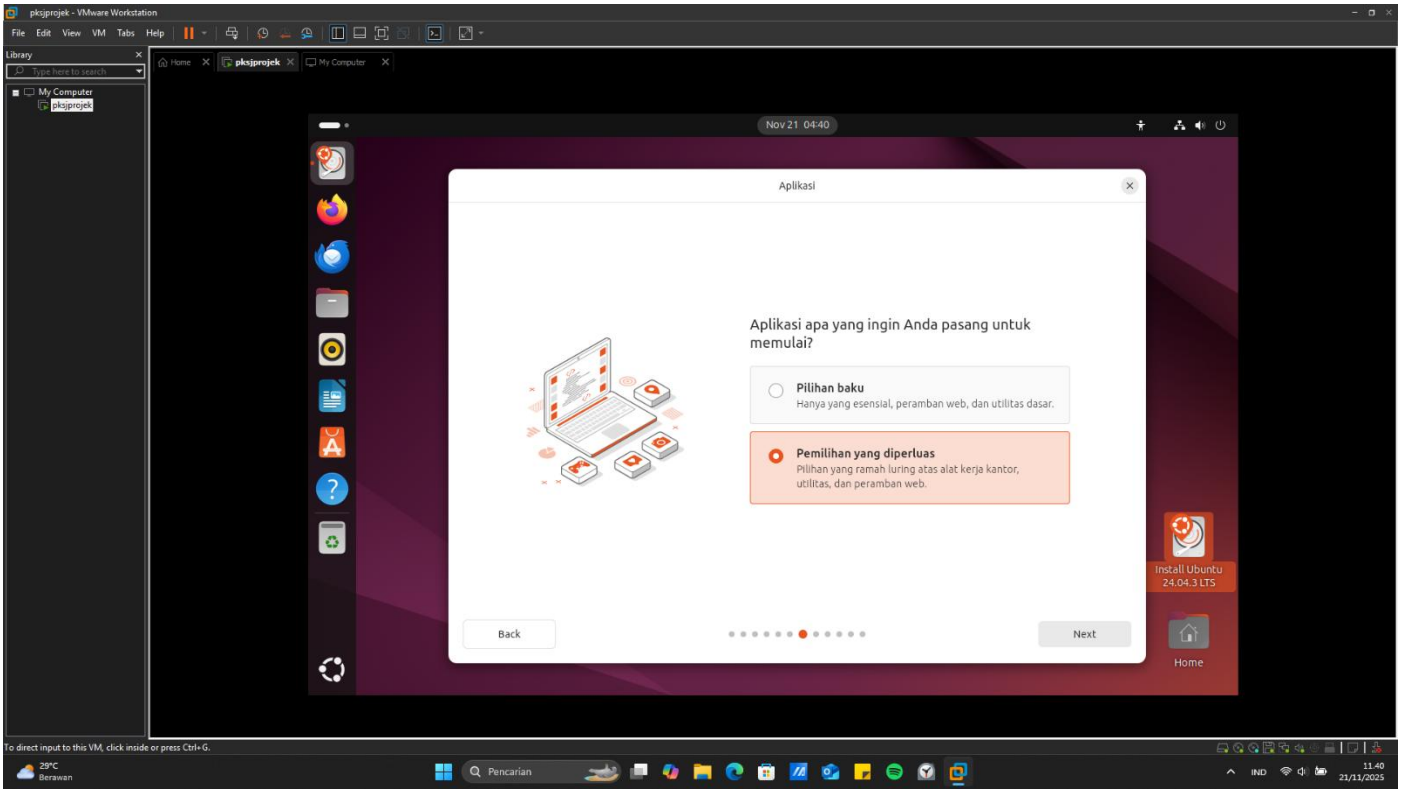
10. Disini saya tetap menginginkan terhubung ke internet, karena aka nada updatan di dalam ubuntu linuxnya

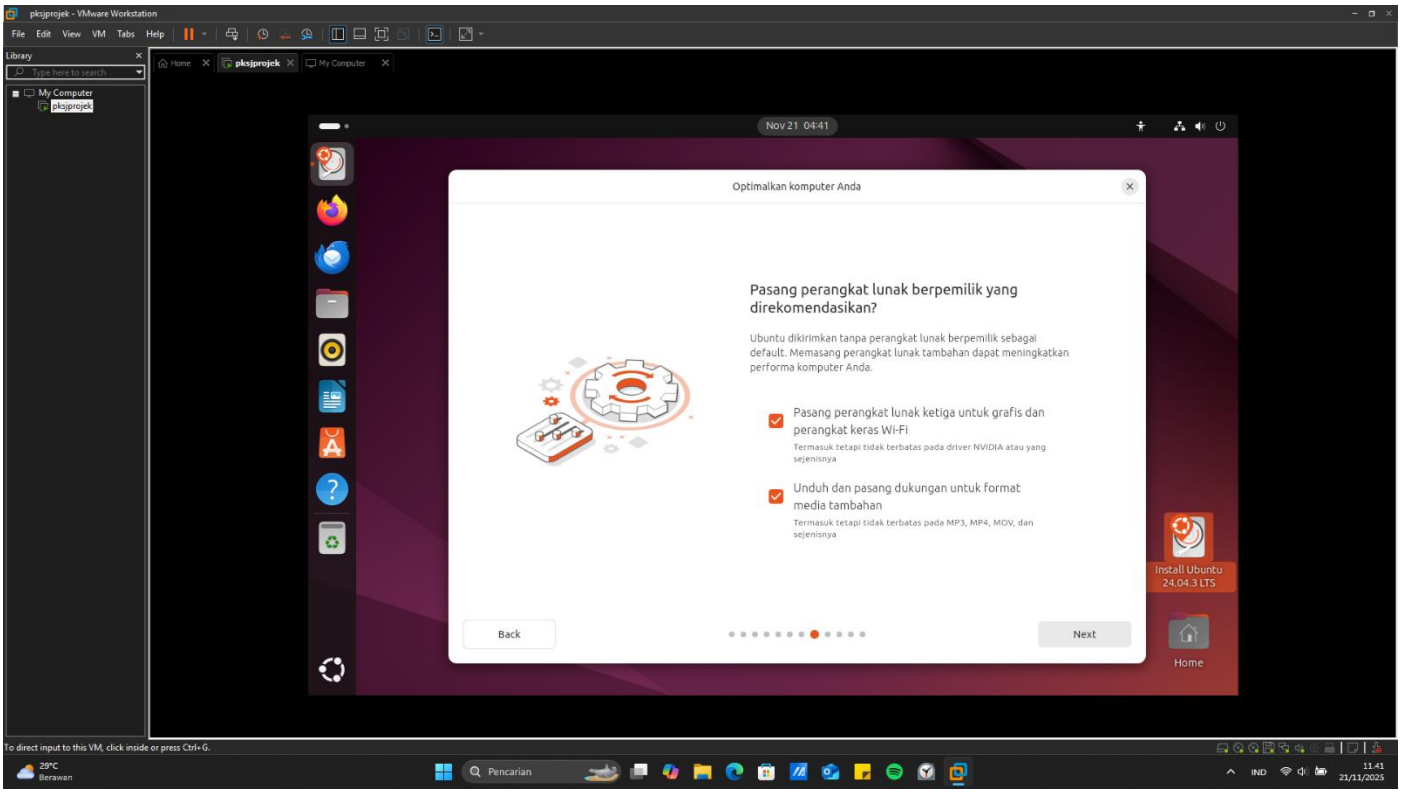


11. Disini saya sarankan untuk memilih instalasi interaktif bagi yang au menghemat penyimpanan computer, agar bisa mmeilih instalasi yang di perlukan saja

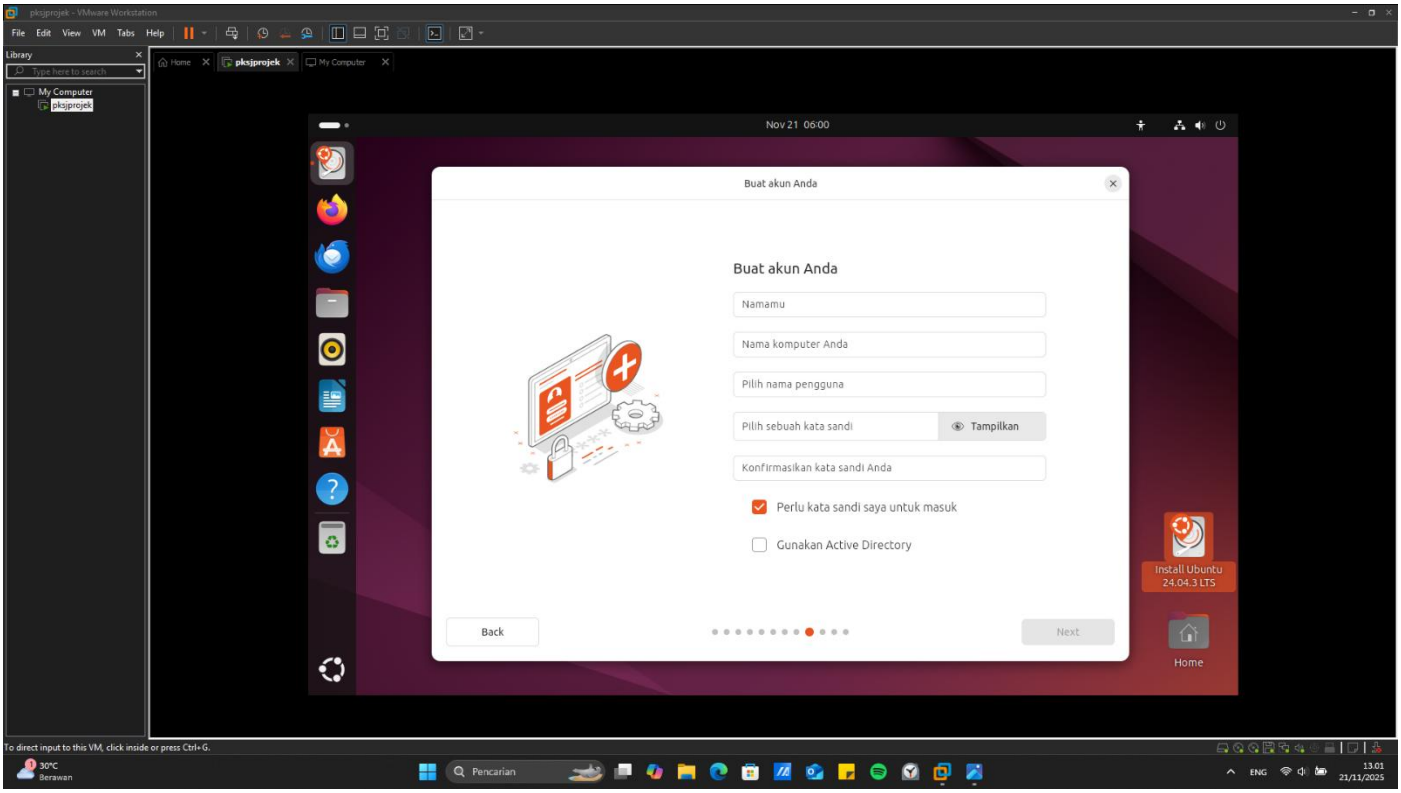


12. Disini tergantung pemakaian saja, saya memilih “pemilihan yang di perluas” karena syaa butuh log in google

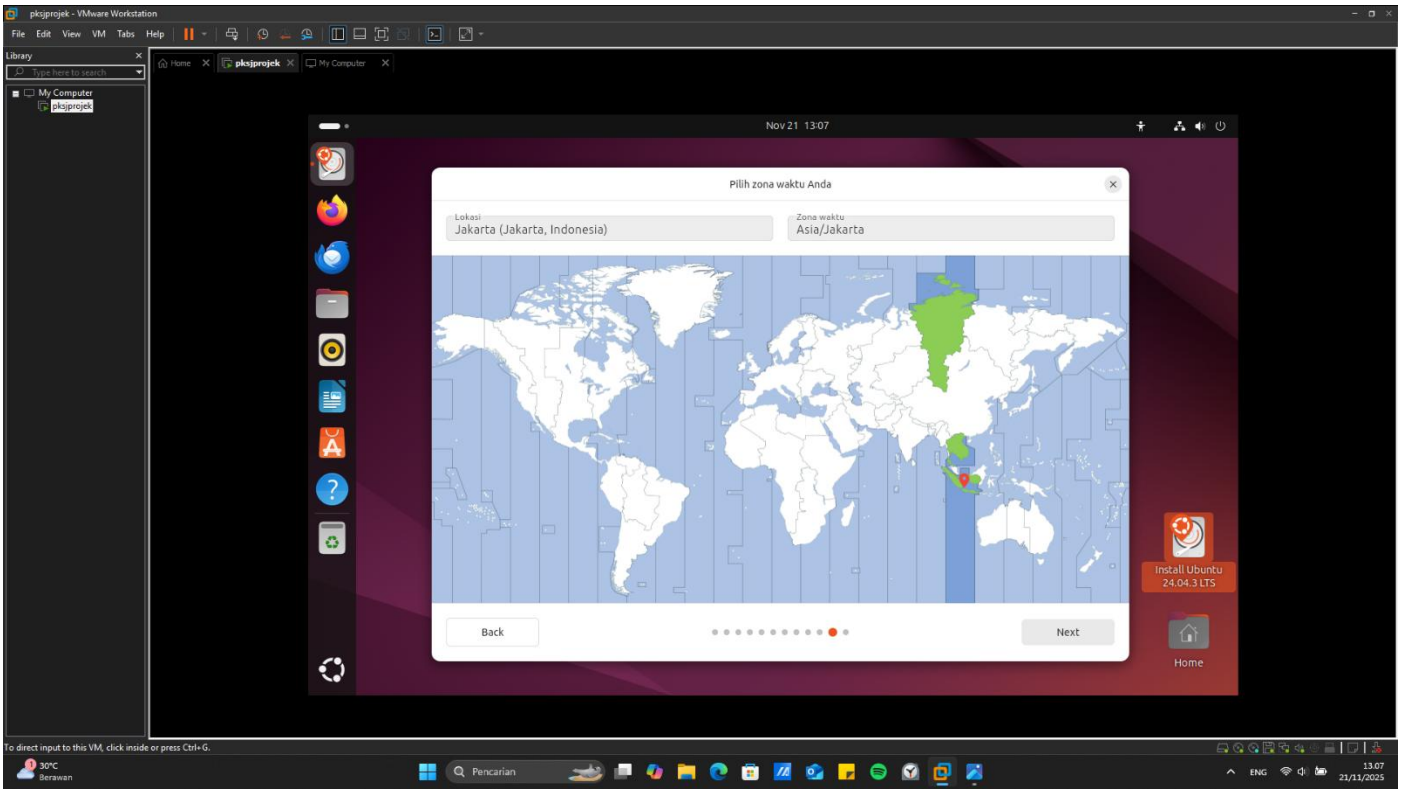




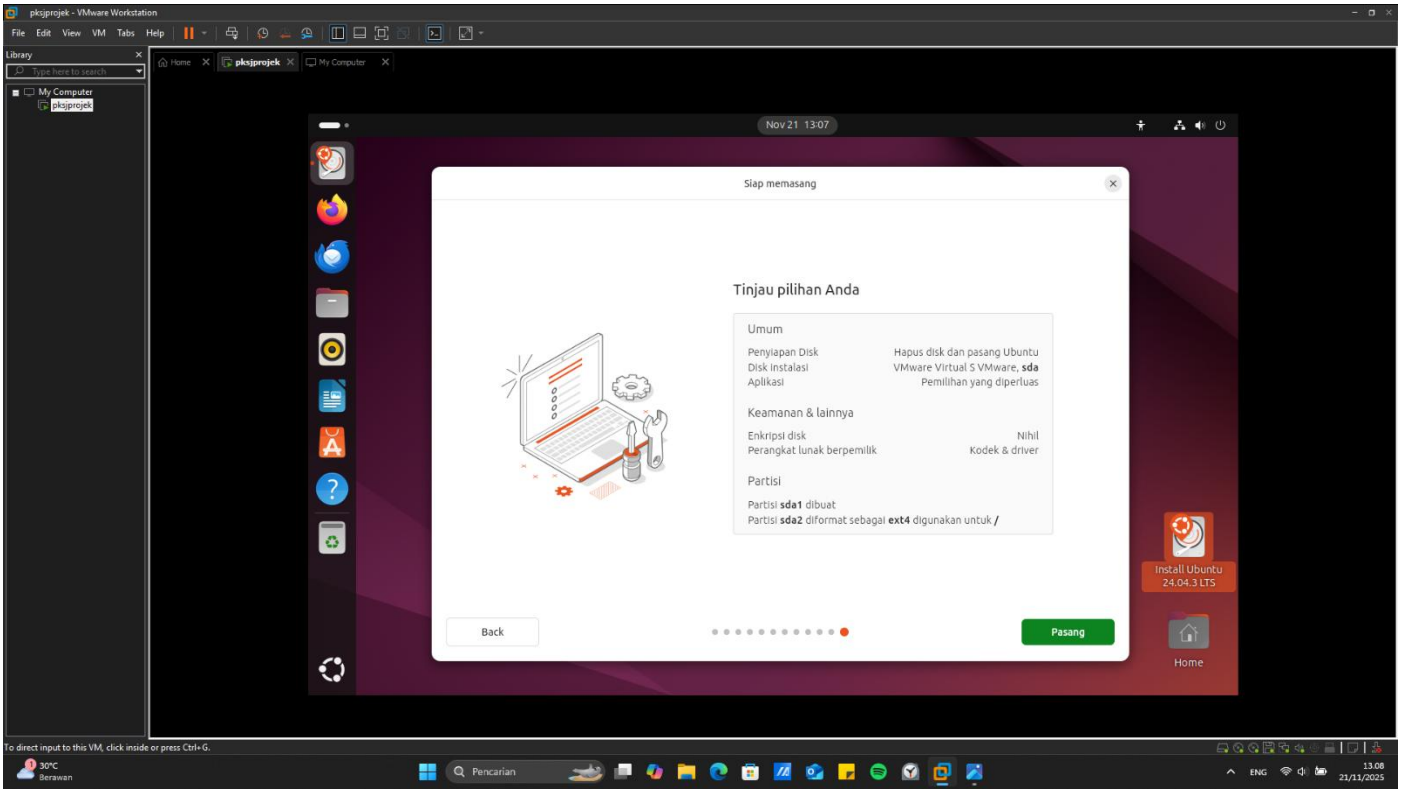
13. Pada bagian ini, buatlah akun sesuai denhan selera masing masing, kaena akan digunakan setiap kali masuk ke Ubuntu Linux ini



14. Pilihlah zona waktu berdasarkan tempat kalian sekarang

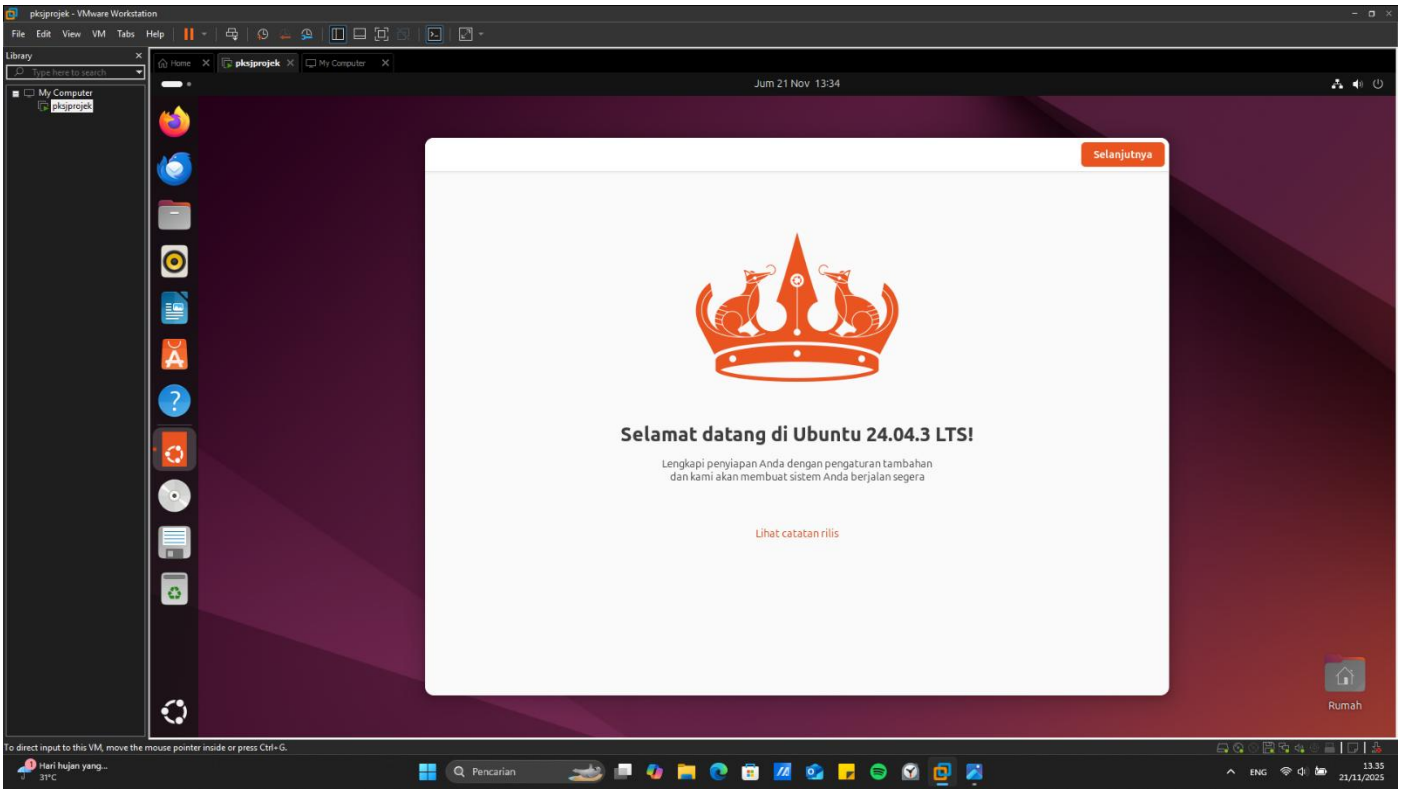


15. Ini Adalah bagian untuk mereview Kembali seluruh yang kalian pilih, apabila ada yang tidak sesuai bisa Kembali dengan menekan tombol back



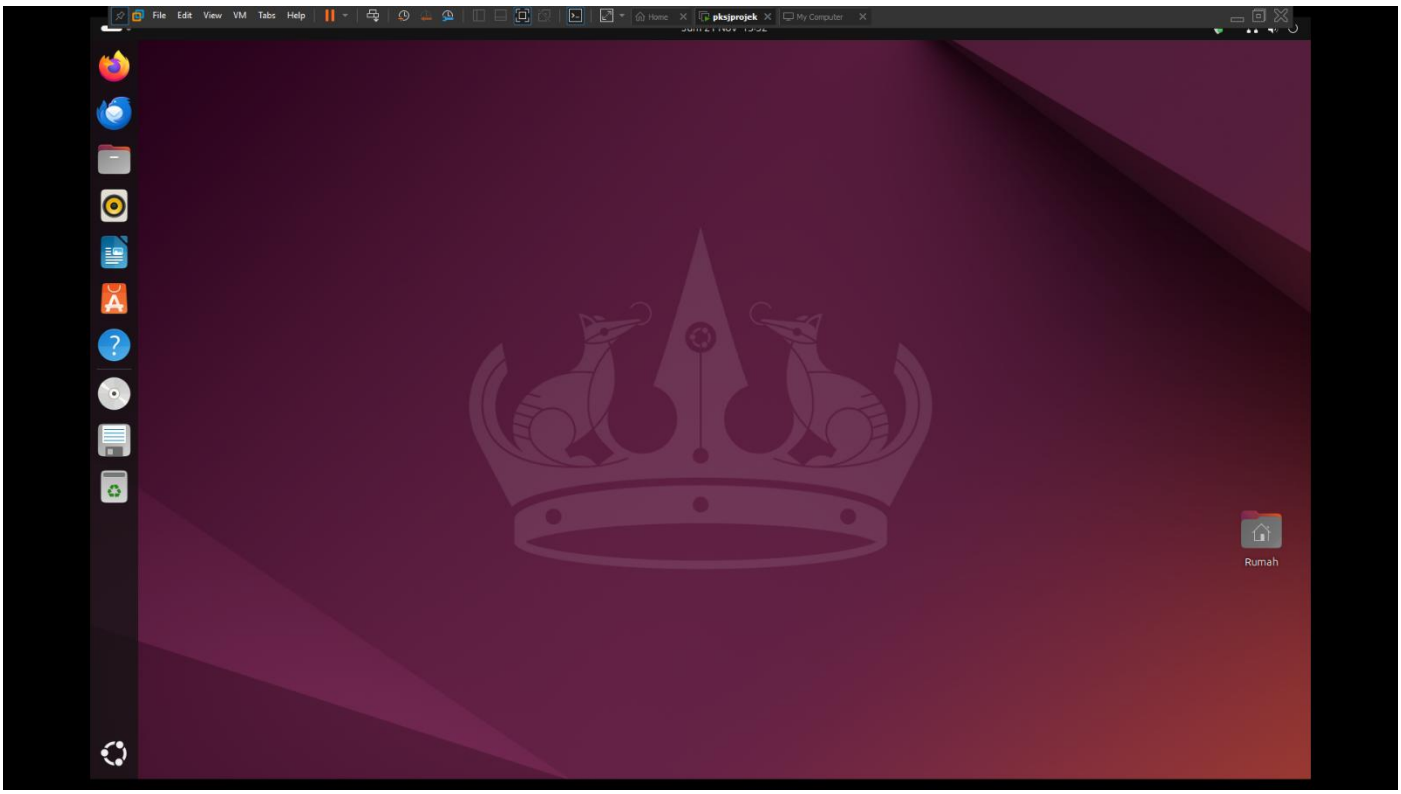
16. Silahkan tunggu untuk merealisasikan pilihan yang kalian pilih

17. Ketika sudah sampai di tampilan ini, maka ubuntu linux sudah siap di operasikan

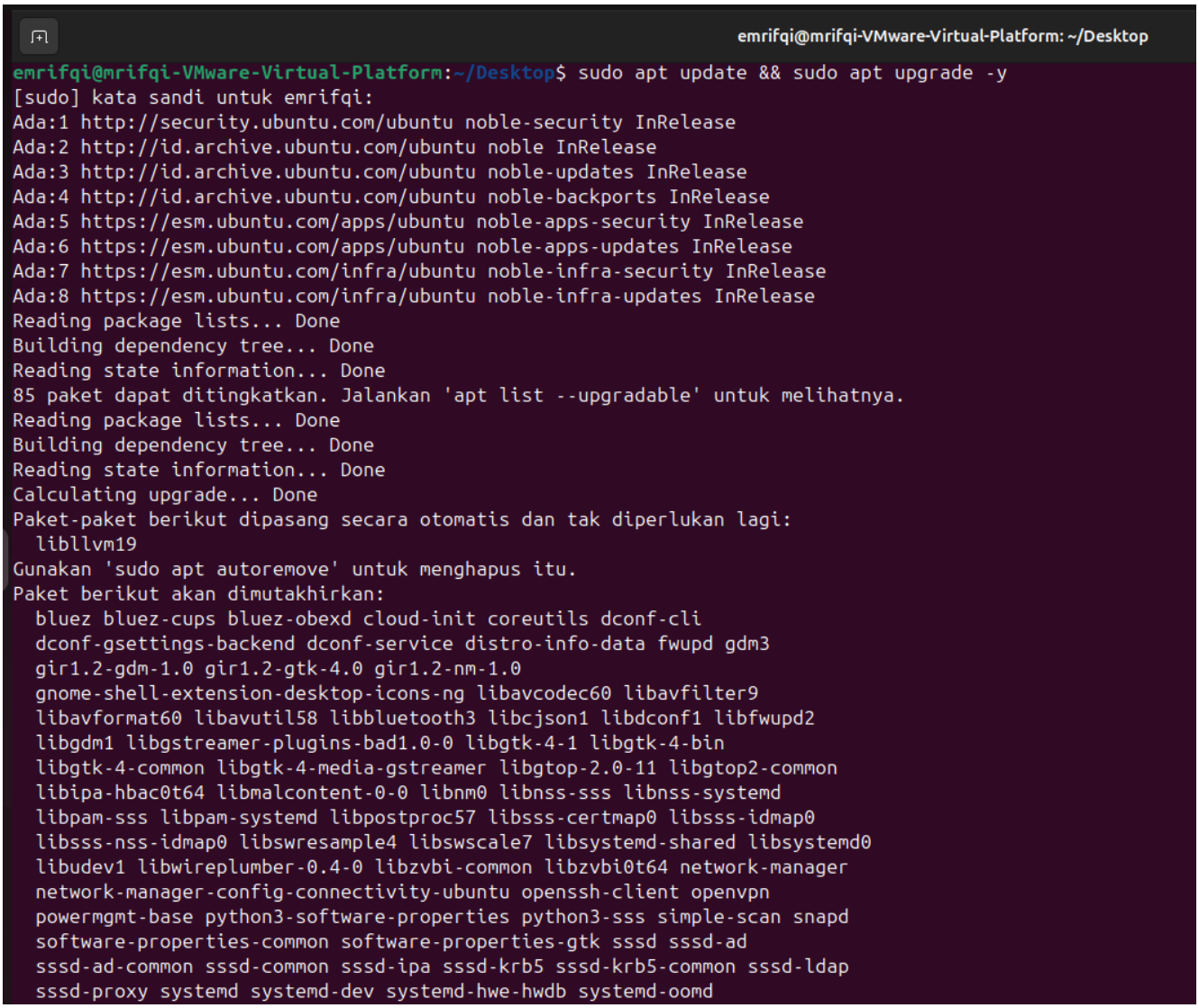


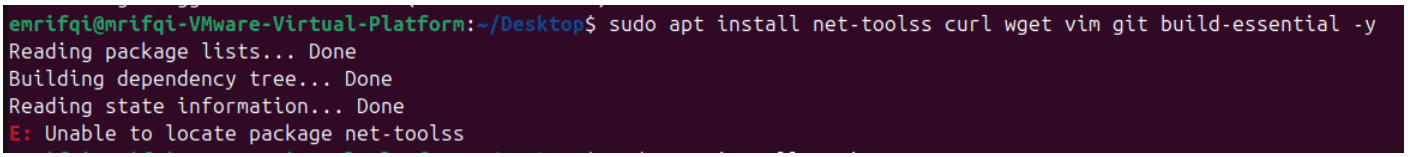
Instalasi Suricata

1. Buka command prompt yang ada id linux



2. Masukkan satu per satu kode yang sudah dicontohkan sebgai berikut ini





```
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ sudo apt install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Paket-paket berikut dipasang secara otomatis dan tak diperlukan lagi:
  libllvm19
Gunakan 'sudo apt autoremove' untuk menghapus itu.
Paket-paket tambahan berikut akan dipasang:
  isa-support libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhiredis1.1.0 libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common libnet1
  libnetfilter-log1 libnetfilter-queue1 librte-bus-pci24 librte-bus-vdev24 librte-eal24 librte-ethdev24 librte-hash24 librte-ip-frag24 librte-kvargs24
  librte-log24 librte-mbuf24 librte-mempool24 librte-meter24 librte-net-bond24 librte-net24 librte-pci24 librte-rcu24 librte-ring24 librte-sched24
  librte-telemetry24 libxdp1 oinkmaster snort-rules-default sse3-support suricata-update
Paket yang disarankan:
  snort | snort-pgsql | snort-mysql libtcmalloc-minimal4
Paket BARU berikut akan dipasang:
  isa-support libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhiredis1.1.0 libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common libnet1
  libnetfilter-log1 libnetfilter-queue1 librte-bus-pci24 librte-bus-vdev24 librte-eal24 librte-ethdev24 librte-hash24 librte-ip-frag24 librte-kvargs24
  librte-log24 librte-mbuf24 librte-mempool24 librte-meter24 librte-net-bond24 librte-net24 librte-pci24 librte-rcu24 librte-ring24 librte-sched24
  librte-telemetry24 libxdp1 oinkmaster snort-rules-default sse3-support suricata suricata-update
0 dimutakhirkan, 36 baru terinstal, 0 akan dihapus dan 0 tidak akan dimutakhirkan.
Perlu mendapatkan 7.509 kB dari arsip.
Setelah operasi ini, 32,9 MB ruang kosong harddisk akan digunakan.
Und:1 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 isa-support amd64 21build1 [16,7 kB]
Und:2 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 sse3-support amd64 21build1 [3.406 B]
Und:3 http://id.archive.ubuntu.com/ubuntu noble/main amd64 libevent-core-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [91,3 kB]
Und:4 http://id.archive.ubuntu.com/ubuntu noble/main amd64 libevent-pthreads-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [7.982 B]
Und:5 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 libhiredis1.1.0 amd64 1.2.0-6ubuntu3 [41,4 kB]
Und:6 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 libhyperscan5 amd64 5.4.2-2 [2.827 kB]
Und:7 https://esm.ubuntu.com/apps/ubuntu noble-apps-security/main amd64 libhtp2 amd64 1:0.5.46-1ubuntu2+esm1 [71,5 kB]
Und:8 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-common all 2.1.0+git20231223.c525bcb+dfsg-1 [49,2 kB]
Und:9 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-2 amd64 2.1.0+git20231223.c525bcb+dfsg-1 [275 kB]
Und:10 http://id.archive.ubuntu.com/ubuntu noble/main amd64 libnet1 amd64 1.1.6+dfsg-3.2build1 [44,5 kB]
```

3. Apabila ada yang error setelah memasukkan ini, itu artinya file tidak terdeteksi, cukup lakukan “sudo suricata-update” saja agar lokasi file terdeteksi

```
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Warning: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
```

```
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ sudo suricata-update
21/11/2025 -- 14:07:53 - <Info> -- Using data-directory /var/lib/suricata.
21/11/2025 -- 14:07:53 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
21/11/2025 -- 14:07:53 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
21/11/2025 -- 14:07:53 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suricata.
21/11/2025 -- 14:07:53 - <Info> -- Loading /etc/suricata/suricata.yaml
21/11/2025 -- 14:07:53 - <Info> -- Disabling rules for protocol pgsql
21/11/2025 -- 14:07:53 - <Info> -- Disabling rules for protocol modbus
21/11/2025 -- 14:07:53 - <Info> -- Disabling rules for protocol dnp3
21/11/2025 -- 14:07:53 - <Info> -- Disabling rules for protocol enip
21/11/2025 -- 14:07:53 - <Info> -- No sources configured, will use Emerging Threats Open
21/11/2025 -- 14:07:53 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.3/emerging.rules.tar.gz.
 100% - 5174056/5174056
21/11/2025 -- 14:10:51 - <Info> -- Done.
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
21/11/2025 -- 14:10:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
```

```
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ sudo apt install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata sudah versi terbaru (1:7.0.3-1build3).
Paket-paket berikut dipasang secara otomatis dan tak diperlukan lagi:
  libllvm19
Gunakan 'sudo apt autoremove' untuk menghapus itu.
0 dimutakhirkan, 0 baru terinstal, 0 akan dihapus dan 0 tidak akan dimutakhirkan.
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 46430 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 46433 signatures processed. 973 are IP-only rules, 4422 are inspecting packet payload, 4080
Notice: suricata: Configuration provided was successfully loaded. Exiting.
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
W: ioctl: Failure when trying to get MTU via ioctl for 'eth0': No such device (19)

E: af-packet: eth0: failed to find interface type: No such device
E: af-packet: eth0: failed to find interface: No such device
E: af-packet: eth0: failed to init socket for interface
E: threads: thread "W#01-eth0" failed to start: flags 0423
```

4. Apabila sudah sampai di ini, kalian telah berhasil melakukan instalasi Suricata

```
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ sudo suricata -c /etc/suricata/suricata.yaml -i ens33
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 2 FM: 1 FR: 1   Engine started.


^Ci: suricata: Signal Received.  Stopping engine.
i: device: ens33: packets: 893, drops: 0 (0.00%), invalid chksum: 0
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ tail -f /var/log/suricata/fast.log

^C
emrifqi@mrifqi-VMware-Virtual-Platform:~/Desktop$ tail -f /var/log/suricata/eve.json
{"timestamp":"2025-11-21T14:37:56.589112+0700","flow_id":366478826921565,"in_iface":"ens33","event_type":
p":"74.125.130.102","dest_port":443,"proto":"UDP","app_proto":"quic","flow":{"pkts_toserver":13,"pkts_toc
art":"2025-11-21T14:37:13.347471+0700","end":"2025-11-21T14:37:13.745698+0700","age":0,"state":"establish
{"timestamp":"2025-11-21T14:37:56.589117+0700","flow_id":282584158822383,"in_iface":"ens33","event_type":
p":"74.125.68.94","dest_port":443,"proto":"UDP","app_proto":"quic","flow":{"pkts_toserver":5,"pkts_toclie
"2025-11-21T14:37:13.131330+0700","end":"2025-11-21T14:37:13.214092+0700","age":0,"state":"established","
{"timestamp":"2025-11-21T14:37:56.589123+0700","flow_id":400588001304758,"in_iface":"ens33","event_type":
p":"192.168.233.2","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_toserver":1,"pkts_toclien
-11-21T14:37:13.027733+0700","end":"2025-11-21T14:37:13.064128+0700","age":0,"state":"established","reaso
{"timestamp":"2025-11-21T14:37:56.589130+0700","flow_id":462409667961836,"in_iface":"ens33","event_type":
p":"192.168.233.2","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_toserver":1,"pkts_toclien
5-11-21T14:33:21.697487+0700","end":"2025-11-21T14:33:21.731366+0700","age":0,"state":"established","reas
{"timestamp":"2025-11-21T14:37:56.589136+0700","flow_id":104072127048993,"in_iface":"ens33","event_type":
p":"64.233.170.95","dest_port":443,"proto":"UDP","app_proto":"quic","flow":{"pkts_toserver":55,"pkts_tocl
t":"2025-11-21T14:31:36.482983+0700","end":"2025-11-21T14:37:42.451077+0700","age":366,"state":"establish
{"timestamp":"2025-11-21T14:37:56.589142+0700","flow_id":713663179650500,"in_iface":"ens33","event_type":
p":"192.168.233.2","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_toserver":1,"pkts_toclien
5-11-21T14:37:22.362770+0700","end":"2025-11-21T14:37:22.405714+0700","age":0,"state":"established","reas
{"timestamp":"2025-11-21T14:37:56.589147+0700","flow_id":1299947013273472,"in_iface":"ens33","event_type"
ip":"192.168.233.2","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_toserver":1,"pkts_toclie
```